
PIEDRA DEL SOL
CASA DE LA CULTURA
FLORIDABLANCA
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
CASA DE LA CULTURA – PIEDRA DEL SOL- 2021

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

| PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PIEDRA DEL SOL CASA DE LA CULTURA DE FLORIDABLANCA. | | |
|---|---|---|
| CIO | | |
| DIRECCIÓN | IDANIA ORTIZ MUÑOZ | |
| TEMA | Plan de Seguridad y Privacidad de la Información. | |
| FECHA DE ELABORACION | Enero 2021 | |
| FORMATO | PDF | |
| VERSIÓN | 01 | |
| **COMITÉ** | **RESOLUCIÓN** | **FECHA** |
| Comité de Dirección | | |

# TABLA DE CONTENIDO.

## 1. INTRODUCCIÓN.

El presente documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para la elaboración del **Plan de Seguridad y Privacidad de la Información de La Casa de la Cultura Piedra Del Sol – Floridablanca.** Para suministrar los requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI basado en la Estrategia de Gobierno en Línea – GEL y el fortalecimiento del modelo TI del estado, del Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidad se busca contribuir al incremento de la transparencia en la gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad digital y la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que servirán para proteger la privacidad de la información y los datos de los procesos de la entidad y las personas vinculadas con dicha información y los usuarios de la entidad.

## 2. JUSTIFICACION.

**La Casa De Cultura Piedra Del Sol – Floridablanca** en acorde y alineada a las políticas del Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI y dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica *El Modelo de Seguridad y Privacidad de la Información*, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea

.

La entidad busca mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabajar en el fortalecimiento de la seguridad de la información en la entidad, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana y sujeto a cambios periódicos de acuerdo a la implementación de este en la entidad o los cambios de legislación que proponga el estado.

## 3. GLOSARIO.

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo En relación con la seguridad de la información**: se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). • Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Cyber seguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701). Ciberespacio Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas** concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad Documento** que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3) • Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar,

responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008. • Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho

que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo Posibilidad** de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto

de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad Cualidad** que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad Debilidad** de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Partes interesadas (Stakeholder**) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## 4. OBJETIVOS.

### 4.1 Objetivo General.

Diseñar, generar e implementar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la entidad alineado al Modelo de Seguridad y Privacidad de la información, al plan de seguridad y privacidad de la información con la finalidad de fortalecer el aseguramiento de los servicios TI y preservar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad y los usuarios.

### 4.2 Objetivo Específicos.

- Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos críticos previamente identificados y las acciones para mitigar el riesgo.

- Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.
- Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
. • Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Establecer en la entidad en la transición de lPv4 a IPv6 con la utilización de las guías disponibles para tal fin. • Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.

## 5. NORMATIVIDAD.

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- **Ley 1437 de 2011, Capítulo IV,** "utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites

administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

- **Ley 1581 de 2012, g) Principio de seguridad** "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento." • Ley 1581 de 2012, Artículo 17, ítem d "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

- **Ley 1712 de 2014, "principio de transparencia"** "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.".

- **Ley 1712 de 2014, artículo 7**: "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- Ley 1712 de 2014 -Título III "Excepciones acceso a la información"

"Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."

- **Decreto 2573 de 2014** "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

- **Decreto 1413 de 2017, artículo 2.2.17.6.6,** "Seguridad de la información." "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

- **Decreto 1413 de 2017, artículo 2.2.17.6.1,** "Responsable y encargado del tratamiento": "Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

- **Decreto 1413 de 2017, artículo 2.2.17.6.3.** Responsabilidad demostrada y programa integral de gestión de datos. los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.

- **Decreto 1413 de 2007, artículo 2.2.17.6.5, "Privacidad por diseño y por defecto" "**Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"

- **Decreto 1413 de 2017, artículo 2.2.17.5.10, "Derechos de los usuarios de los servicios ciudadanos digitales**"

- Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.
- Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.
- Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.
- Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.
- Elegir y cambiar libremente el operador de servicios ciudadanos digitales.
- Solicitar en cualquier momento, y a través de cualquiera de los medios de atención
- al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.

- **Decreto 1413 de 2017, artículo 2.2.17.2.1.1 "Descripción de los**

**servicios ciudadanos digitales**, 1.5 servicio de interoperabilidad Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicas cuando lo requieran."

- **Decreto 612 de 2018, artículo 1. "Integración de planes institucionales y estratégico.** Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

## 6.MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El modelo de seguridad y privacidad de la información de la entidad contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. Se muestra el funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la entidad.

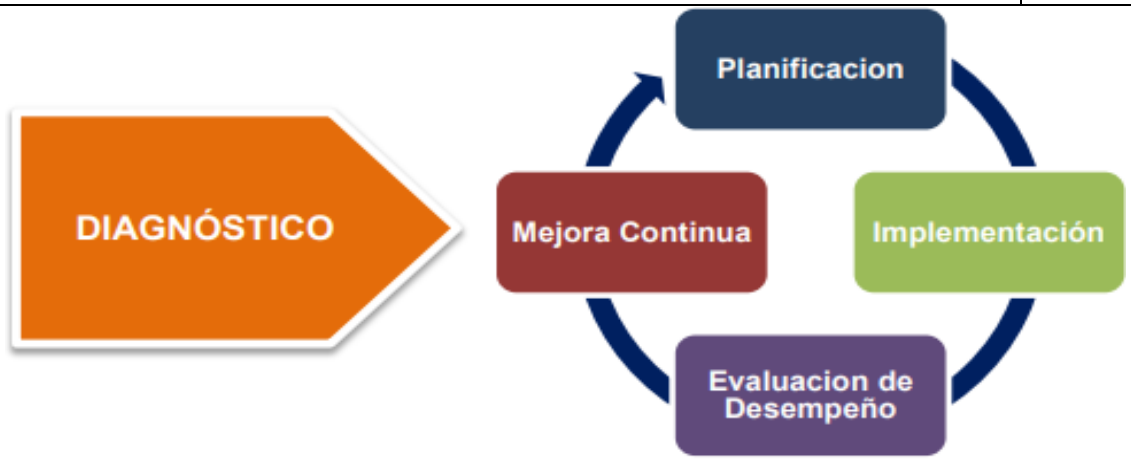


Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

**Fuente:** Guía Modelo de Seguridad y Privacidad de la Información

### 6.1 FASE DIAGNOSTICA.

En esta fase se pretende identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.


Figura 2 – Etapas previas a la implementación

**Fuente:** Guía Modelo de Seguridad y Privacidad de la Información

Tabla 1 -[1.] Metas, Resultados e Instrumentos de la fase etapas previas a la implementación:

| PASOS PAR EL DIAGNOSTICO DE SEGURIDAD Y PRIVACIDAD. CASA DE LA CULTURA PIEDRA DEL SOL. FLORIDABLANCA. | | | |
|---|---|---|---|
| METAS | RESULTADOS | INSTRUMENTOS MSPI. | ALINEACIÓN MRAE. |
| Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. | Diligenciamiento de la herramienta. | Herramienta de diagnóstico.<br>• Instructivo para el diligenciamiento de la herramienta. | LI.ES.01<br>LI.ES.02<br>LI.GO.01<br>LI.GO.04<br>LI.GO.05<br>LI.GO.07 |

| | | | |
|---|---|---|---|
| Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad | Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad. | • Guía No 1 - Metodología de Pruebas de Efectividad | LI.ST.14 |
| Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. | Documento con los hallazgos encontrados en las pruebas de vulnerabilidad. | | |

**MRAE:** Marco de referencia arquitectura TI. **MSPI:** Modelo de seguridad y protección de la seguridad.

Para realizar dicha fase las entidad deben efectuar la recolección de la información con la ayuda de *la herramienta de diagnóstico y la metodología de pruebas de efectividad* (https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf).

**En la fase de diagnóstico** del MSPI se pretende alcanzar las siguientes **metas**:

-Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.

- Determinar el nivel de madurez de los controles de seguridad de la información.

- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

-Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

- Identificación del uso de buenas prácticas en cyber seguridad.

## 6.2 FASE DE PLANIFICACIÓN.

En esta fase la entidad deberá utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

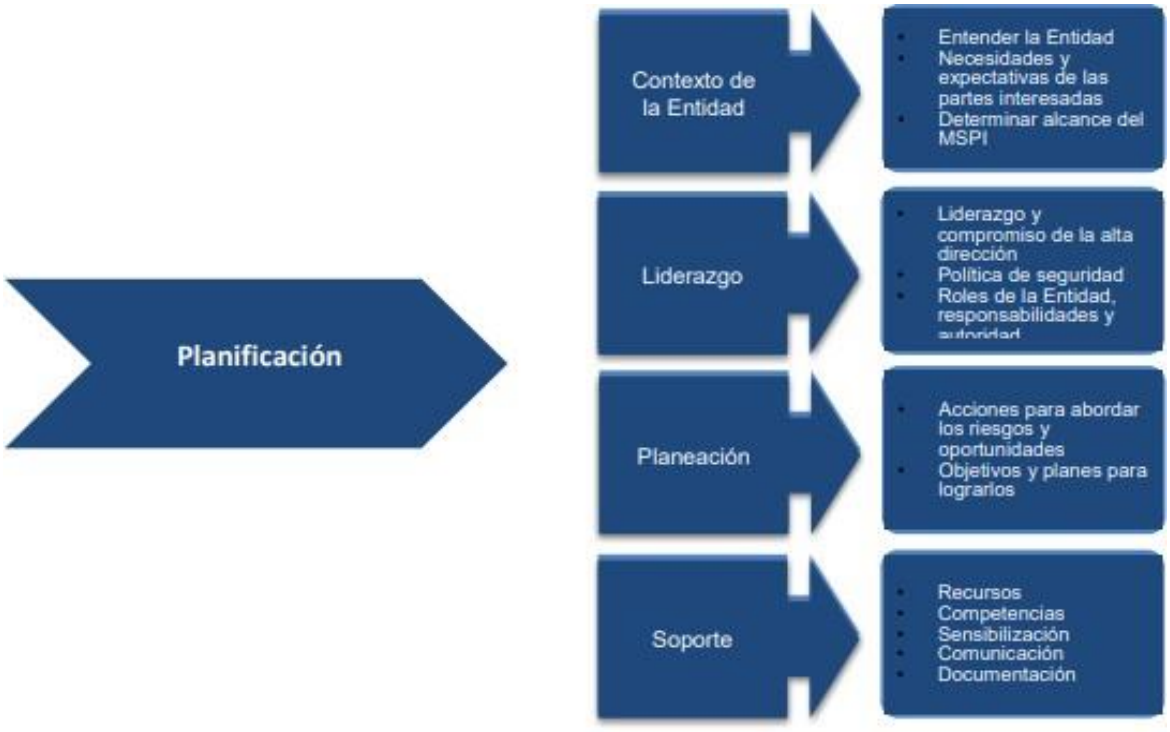


Figura 3 - Fase de planificación[1]

**Fuente:** Guía Modelo de Seguridad y Privacidad de la Información

Tabla 2 – [1]Plan de acción fase planificación: Metas, Resultados e Instrumentos de la Fase de Planificación.

| FASE DE PLANIFICACIÒN DEL MSPI | | | |
|---|---|---|---|
| **METAS** | **RESULTADOS** | **INSTRUMENTOS MSPI** | **MRAE** |
| Política de Seguridad y privacidad de la información. | Documentos con la Política de Seguridad y privacidad de la información aprobado por la alta Dirección y socializada al interior de la entidad.<br>Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad. | Guía No. 2 Política General MSPI | LI.ES.02<br>LI.ES.06<br>LI.ES.07<br>LI.ES.08<br>LI.ES.09<br>LI.ES.10<br>LI.ES.01<br>LI.ES.04<br>LI.ES.07<br>LI.ES.08<br>LI.ES.09<br>LI.ES.10<br>LI.ES.01<br>LI.ES.02<br>LI.ES.09<br>LI.ES.10<br>LI.ES.11 |
| Procedimientos de seguridad de la información. | Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional | Guía No 3 Procedimientos de Seguridad y privacidad de la información | LI.INF.14<br>LI.SIS.22<br>LI.SIS.23<br>LI.SIS.01<br>LI.ST.05<br>LI.ST.06<br>LI.ST.09<br>LI.ST.10<br>LI.ST.12<br>LI.ST.13<br>LI.ST.14<br>LI.UA.01 |

| | | | |
|---|---|---|---|
| Roles y Responsabilidades de Seguridad y privacidad de la Información | Acto administrativo a través del cual se crea o se modifica las funciones de comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. | Guía No 4 Roles y Responsabilidades de Seguridad y privacidad de la Información | LI.UA.02 LI.UA.03 |
| Inventario de activos de información. | Seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. - Matriz con la identificación valoración y clasificación de activos de información. -Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6 | Guía No 5 Gestión De Activos Guía No 20 Transición Ipv4 a Ipv6 | |
| Integración del MSPI con el sistema de gestión documental | Integración del MSPI con el sistema de gestión documental | Guía No 6 Gestión Documental | |

| | | | |
|---|---|---|---|
| Identificación Valoración y tratamiento de riesgos | Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos Documento con la declaración de aplicabilidad. De documentos revisados y aprobados por la alta Dirección. | Plan de riesgo de la entidad en seguridad y privacidad de la información. Guía No 7 - Gestión de Riesgos Guía No. 8 Controles de Seguridad | |
| Plan de Comunicaciones. | Documento con el plan de comunicación, sensibilización | Guía No 14 Plan de comunicación sensibilización y capacitación | |
| Plan de diagnóstico de IPv4 a IPv6. | Documento con el plan de diagnóstico para la transición del IPv4 a IPv6 | Guía No. 20 Transición IPv4 a IPv6. | |

Las guías herramientas se direccionan o se consiguen en la página fortalecimiento de la gestión TI del estado https://www.mintic.gov.co/gestionti/615/w3- propertyvalue-7275.html.

1 El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

### 6.3. FASE DE IMPLEMENTACIÓN.

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

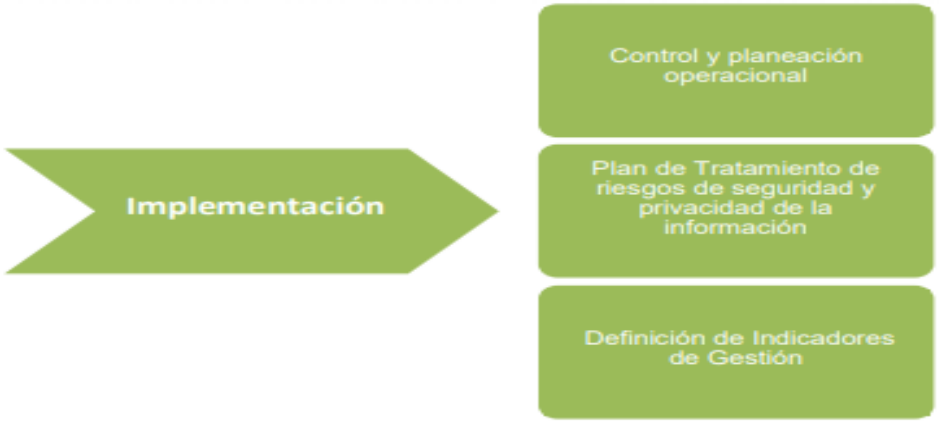


Figura 4 - Fase de implementación[2]

**Fuente:** Guía Modelo de Seguridad y Privacidad de la Información

Tabla: Plan para las fases de implementación.

| PLAN PARA LA IMPLEMENTACIÓN. | | | |
|---|---|---|---|
| **METAS.** | **RESULTADOS.** | **INSTRUMENTOS** | |
| | | **MSPI.** | **MRAE.** |
| Planificación y Control Operacional. | Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. | Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. | LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 . |
| Implementación del plan de tratamiento de riesgos. | Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. | Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos | |
| Indicadores De Gestión | Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. | Guía No 9 - Indicadores de Gestión SI. | LI.ST.06 LI.ST.09 LI.ST.10 LI.ST 12 LI.ST.13 |

| | | | |
|---|---|---|---|
| Plan de Transición de IPv4 a IPv6 | Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6. | LI.UA.01 |

2 El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI.

## 6.4 FASE DE EVALUACIÓN DE DESEMPEÑO.

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

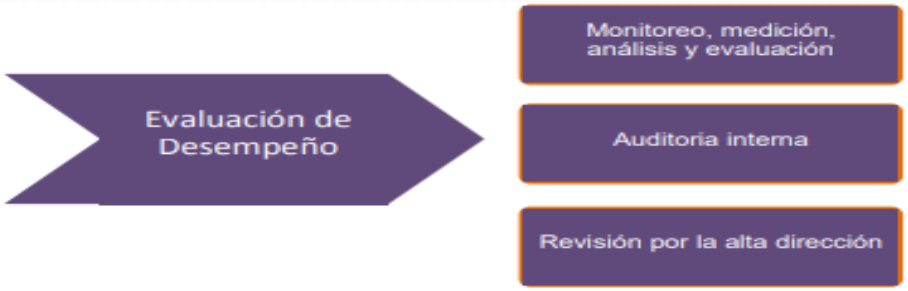


Figura 5 - Fase de Evaluación de desempeño[3]

**Fuente:** Guía Modelo de Seguridad y Privacidad de la Información

Tabla 4 - [2]Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

| Evaluación del Desempeño | | | |
|---|---|---|---|
| Metas | Resultados | Instrumentos | |
| | | MSPI | MRAE |
| Plan de revisión y seguimiento, a la implementación del MSPI. | Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. | Guía No 16 – Evaluación del desempeño. | LI.ES.12<br>LI.ES.13<br>LI.GO.03<br>LI.GO.11<br>LI.GO.12<br>LI.INF.09<br>LI.INF.11<br>LI.INF.13<br>LI.INF.14<br>LI.INF.15<br>LI.SIS.23<br>LI.ST.05<br>LI.ST.06<br>LI.ST.08<br>LI.ST.15<br>LI.UA.07<br>LI.UA.08 |
| Plan de Ejecución de Auditorias | Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección. | Guía No 15 – Guía de Auditoría. | |

## 6.5. FASE DE MEJORA CONTINUA.

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.


Figura 6 - Fase de mejoramiento continúo[4]

Tabla 5 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

| Mejora Continua | | | |
|---|---|---|---|
| Metas | Resultados | Instrumentos | |
| | | MSPI | MRAE |
| Plan de mejora continua | Documento con el plan de mejoramiento.<br><br>Documento con el plan de comunicación de resultados. | Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI.<br><br>Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.<br><br>Guía No 17 – Mejora Continua | LI.GO.03<br>LI.GO.12<br>LI.GO.13<br>LI.INF.14<br>LI.INF.15<br>LI.ST.15<br>LI.UA.9<br>LI.UA.10 |

2 El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001.

En esta fase es importante que la entidad definirá y ejecutara el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.

- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Utilizando los insumos anteriores, la entidad

La entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad.

La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

La guía No 17 - Mejora Continua, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

## 7 ADOPCIÓN DEL PROTOCOLO IPV6.

Para cumplir el objetivo de innovación tecnológica debe iniciar el proceso del protocolo IPv4 al nuevo Protocolo IPv6, para esto se debe revisar que la infraestructura con la que cuenta actualmente soporte el protocolo IPv6, en caso de no ser así realizar cambio de ella. Garantizar que todos los equipos de telecomunicaciones acepten en un 100% este protocolo. Además, en lo relacionado con los proveedores de servicios de conectividad deben proveerlo con total compatibilidad a IPv6. La infraestructura nueva debe estar diseñada para coexistir con el protocolo IPv4. 9. Guías Modelo de Seguridad y Privacidad de la Información Los siguientes documentos brindados por el MINTIC serán tenidos en cuenta en la implementación el Modelo de Seguridad y Privacidad de la entidad.

La entidad se regirá por las siguientes Guías No 20 – Transición IPv4 a IPv6. Guía No 19 – Aseguramiento del protocolo IPv6. Circular 002 de 2011 del Min TIC.

**Guías Modelo de Seguridad y Privacidad de la Información**
Los siguientes documentos brindados por el MINTIC serán tenidos en cuenta en la implementación el Modelo de Seguridad y Privacidad de la Información

| Modelo de Seguridad y Privacidad de la Información | |
|---|---|
| **Instructivo Herramienta de Diagnostico** | |
| **Herramienta de Diagnostico** | |
| **Guía Mi pymes** | |
| Guía 1 | Metodología de pruebas de efectividad |
| Guía 2 | Política General MSPI v1 |
| Guía 3 | Procedimientos de Seguridad y Privacidad de la Información |
| Guía 4 | Roles y responsabilidades de seguridad y privacidad de la información |
| Guía 5 | Gestión de Activos |
| Guía 6 | Gestión Documental |
| Guía 7 | Gestión de Riesgos |
| Guía 8 | Controles de Seguridad |
| Guía 9 | Indicadores Gestión SI |
| Guía 10 | Continuidad de TI |
| Guía 11 | Impacto Negocio |
| Guía 12 | Seguridad en la Nube |
| Guía 13 | Guía De Evidencia Digital |
| Guía 14 | Plan de comunicación, sensibilización y capacitación |
| Guía 15 | Auditoria |
| Guía 16 | Evaluación del Desempeño |
| Guía 17 | Mejora Continua |

## 8 PRIVACIDAD DE LA INFORMACIÓN.

Esta Presenta las mismas fases de la seguridad de la información. Pero la entidad deberá desarrollarla siguiendo lo establecido en la Guía sobre Instrumentos de Gestión de la Información Pública de la Secretaría de Transparencia de la Presidencia de la República y las guías modelos de privacidad de la información.

## 9 PLAN DE COMUNICACIÓN

El Plan de seguridad y privacidad de la información, será comunicado a todos los funcionarios de la administración a través de los mecanismos como son Portal Web Territorial donde se publicará en el canal de transparencia y derecho de acceso a la información pública para que todos los usuarios puedan acceder, se enviara a través de correo electrónico a todos los funcionarios de la entidad.

## 10 BIBLIOGRAFIA.

**1.** Guía para la gestión del modelo de seguridad de la información, Min TIC. 2 - Norma técnica colombiana ISO 27001:2013.
3. Guías fortalecimiento TI, **/www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.**

FIRMADO EL VENTIUNO (21) DE ENERO DEL 2021

**IDANIA ORTIZ MUÑOZ**
**Directora General**
**CASA DE LA CULTURA PIEDRA DEL SOL**

PROYECTO: JUAN MANUEL RAMIREZ – TESORERO GENERAL.

# RESOLUCIÓN No. 19 DE ENERO DEL 2021

**"POR MEDIO DEL CUAL SE ADOPTA DURANTE LA VIGENCIA 2021, EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA CASA DE LA CULTURA PIEDRA DEL SOL DE FLORIDABLANCA – SANTANDER"**

La Directora de la Casa de la Cultura Piedra del Sol de Floridablanca, Santander, es uso de sus atribuciones constitucionales y legales y en especial las conferidas por la ley 909 de 2004 y Decreto 1785 de 2014.

## CONSIDERANDO:

Que la Ley 1437 de 2011, Capítulo IV, en su tenor literal señala: "utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos".

Que la Ley 1581 de 2012, g) Principio de seguridad establece que "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Del mismo modo, en su artículo 17, ítem d "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

La Ley 1712 de 2014, por medio del cual se establece el "principio de transparencia" "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley".

Por su parte, el artículo 7 *ibídem*, señala la "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten".

Que el Título III de la Ley 1712 de 2014 - "Excepciones acceso a la información" "Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito".

Que el Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

El artículo 2.2.17.6.6. del Decreto 1413 de 2017 "Seguridad de la información", en su tenor literal señala: "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información".

Del mismo modo, el artículo 2.2.17.6.1 *ibidem*, "Responsable y encargado del tratamiento", señala que: "Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen".

Que el artículo 2.2.17.6.3 *ibidem* señala la Responsabilidad demostrada y programa integral de gestión de datos. Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.

Que los artículos 2.2.17.6.5, 2.2.17.5.10 y 2.2.17.2.1.1 del Decreto 1413 de 2017, establece la **"**Privacidad por diseño y por defecto", los "Derechos de los usuarios de los servicios ciudadanos digitales" y la "Descripción de los servicios ciudadanos digitales.

Por último, el Decreto 612 de 2018 en su artículo 1, establece la "Integración de planes institucionales y estratégico", y entre ellos se encuentra "El Plan de Seguridad y Privacidad de la Información; por ende, las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos y publicarlo en su respectiva página web.

**RESUELVE:**

**ARTÍCULO PRIMERO:** Adoptar el plan de seguridad y privacidad de la información para el año 2021 de la Casa de la Cultura Piedra del Sol, cuyo texto se anexa a la presente Resolución.
**ARTÌCULO SEGUNDO**: El plan de seguridad y privacidad de la información, queda supeditado en su ejecución a la disponibilidad presupuestal del rubro correspondiente para la presente vigencia.

**COMUNÍQUESE Y CUMPLASE**
Dado en Floridablanca a los veintiún (21) días de enero de 2021

**IDANIA ORTIZ MUÑOZ**
**Directora General**
**CASA DE LA CULTURA PIEDRA DEL SOL**

PROYECTO: JUAN MANUEL RAMIREZ – TESORERO GENERAL